WE CLAIM:

1. An information security policy evaluation system comprising:

a first information processing apparatus located on a first site;

a second information processing apparatus located on a second site; and

a third information processing apparatus located on a third site,

the first through the third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a treated threat data storage section for storing treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus has a treated threat data transmission section for transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus has a threat data transmission section for transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a treated threat data reception section for receiving the treated threat data and a threat data reception section for receiving the threat data,

the first information processing apparatus has a

correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and the treated threat data, and

the first information processing apparatus has an effective treated threat data extraction section for extracting a piece of treated threat data to which there is a piece of threat data corresponding in the threat data received by the threat data reception section, out of the treated threat data received by the treated threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted treated threat data is described.

2. An information security policy evaluation system comprising:

a first information processing apparatus located on a first site;

a second information processing apparatus located on a second site; and

a third information processing apparatus located on a third site,

the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a treated threat data storage section for storing treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus has a treated threat data transmission section for transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus has a threat data transmission section for transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a treated threat data reception section for receiving the treated threat data and a threat data reception section for receiving the threat data,

the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and the treated threat data, and

the first information processing apparatus has an untreated threat data extraction section for extracting a piece of threat data to which there is no piece of treated threat data corresponding in the treated threat data received by the treated threat data reception section, out of the threat data received by the threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted threat data is described.

3. The information security policy evaluation system according to claim 1,

wherein the first information processing apparatus has a loss amount data storage section for storing loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat, and

the evaluation data generation section has an effect order

sort section for generating the evaluation data in which the treated threat data extracted by the effective treated threat data extraction section is sorted and described in descending order of the loss amount data of the threat data related to the respective treated threat data in the correspondence data.

4. The information security policy evaluation system according to claim 1,

wherein the first information processing apparatus has a loss amount data storage section for storing loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat, and

the evaluation data generation section has a consideration priority sort section for generating the evaluation data in which the threat data extracted by the untreated threat data extraction section is sorted and described in descending order of the loss amount data.

5. The information security policy evaluation system according to claim 3,

wherein the threat data transmission section of the third information processing apparatus attaches the loss amount data to the threat data and transmits the loss amount data to the first information processing apparatus,

the threat data reception section of the first information processing apparatus receives the loss amount data as well as the threat data, and

the loss amount data storage section of the first information processing apparatus stores the received loss amount data.

6. The information security policy evaluation system according to claim 1, wherein the third information processing apparatus has a threat data update section for updating the threat data and, the threat data transmission section transmits the updated threat data to the first information processing apparatus in a case where the threat data has been updated by the threat data update section.

7. The information security policy evaluation system according to claim 1, further comprising:

an evaluation result output section for displaying contents of the evaluation data generated by the evaluation data generation section on a display and/or printing the contents of the evaluation data generated by the evaluation data generation section by using a printer.

8. The information security policy evaluation system according to claim 1, further comprising:

a fourth information processing apparatus located on a fourth site, the fourth information processing apparatus being communicably connected to the first to third information processing apparatuses,

wherein the fourth information processing apparatus has a compensation amount storage section for storing a compensation amount of insurance which an organization operating the second site has taken out and which compensates a loss occurring in a case where damage due to a threat is suffered,

the first information processing apparatus has an evaluation data transmission section for transmitting the evaluation data generated by the evaluation data generation

section to the fourth information processing apparatus,

the fourth information processing apparatus has an evaluation data reception section for receiving the evaluation data, and

the fourth information processing apparatus has a compensation amount setting section for resetting the stored compensation amount to the compensation amount determined in accordance with the evaluation data received by the evaluation data reception section.

9. The information security policy evaluation system according to claim 1,

wherein the second site is a site of a customer who requests evaluation of the information security policy,

the third site is a site of a threat information provider who provides threat information, the threat information provider collecting information on threats and providing the information, and

the first site is a site of an evaluator who evaluates the information security policy operated on the second site in compliance with a request from the customer.

10. The information security policy evaluation system according to claim 8,

wherein the second site is a site of a customer who requests evaluation of the information security policy,

the third site is a site of a threat information provider who provides threat information, the threat information provider collecting information on threats and providing the information,

the first site is a site of an evaluator who evaluates the information security policy operated on the second site in

compliance with a request from the customer,

the fourth site is a site of an insurer running an insurance service in which a subscriber is the customer and in which a product is insurance for compensating for a loss occurring in a case where the second site has suffered a threat,

the customer pays the evaluator an evaluation fee for requesting evaluation of the information security policy,

the evaluator receives the evaluation fee from the customer,

the evaluator pays the threat information provider part of the received evaluation fee as an information fee,

the evaluator pays the insurer part of the received evaluation fee as a premium which the customer pays for the insurance, instead of changing the compensation amount,

the customer pays the insurer a premium for the insurance, and

the insurer determines the compensation amount in accordance with the evaluation data.

11. The information security policy evaluation system according to claim 10, wherein any one of the evaluator and the insurer creates an audit report resulting from an audit as to whether the customer appropriately performs operation in accordance with the information security policy, and determines the compensation amount in compliance with the audit report.

12. The information security policy evaluation system according to claim 8, wherein the fourth information processing apparatus is located on the first site and operated by the same organization as that operating the first information processing apparatus.

13. An information security policy evaluation system comprising:

a first information processing apparatus located on a first site;

a second information processing apparatus located on a second site; and

a third information processing apparatus located on a third site,

the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a policy data storage section for storing policy data which is data indicating an information security policy operated on the second site,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus has a policy data transmission section for transmitting the policy data to the first information processing apparatus,

the third information processing apparatus has a threat data transmission section for transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a policy data reception section for receiving the policy data and a threat data reception section for receiving the threat data,

the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and policy data indicating an effective information security

policy against a threat indicated by the threat data, and

the first information processing apparatus has an effective policy data extraction section for extracting a piece of policy data to which there is a piece of threat data corresponding in the threat data received by the threat data reception section, out of the policy data received by the policy data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted policy data is described.

14. An information security policy evaluation system comprising:

a first information processing apparatus located on a first site;

a second information processing apparatus located on a second site; and

a third information processing apparatus located on a third site,

the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a policy data storage section for storing policy data which is data indicating an information security policy operated on the second site,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus has a policy data transmission section for transmitting the policy data to the first information processing apparatus,

the third information processing apparatus has a threat

data transmission section for transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a policy data reception section for receiving the policy data and a threat data reception section for receiving the threat data,

the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and policy data indicating an effective information security policy against a threat indicated by the threat data, and

the first information processing apparatus has an untreated threat data extraction section for extracting a piece of threat data to which there is no piece of policy data corresponding in the policy data received by the policy data reception section, out of the threat data received by the threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted threat data is described.

15. A method of controlling an information security policy evaluation system having a first information processing apparatus located on a first site, a second information processing apparatus located on a second site, and a third information processing apparatus located on a third site, the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus stores treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus stores threat

data which is data indicating a threat having occurred in a past,

the second information processing apparatus transmits the treated threat data to the first information processing apparatus,

the third information processing apparatus transmits the threat data to the first information processing apparatus,

the first information processing apparatus receives the treated threat data and the threat data,

the first information processing apparatus stores correspondence data which is data indicating correspondence between the threat data and the treated threat data, and

the first information processing apparatus extracts a piece of treated threat data to which there is a piece of threat data corresponding in the received threat data, out of the received treated threat data based on the correspondence data, and generates evaluation data in which the extracted treated threat data is described.

16. A method of controlling an information security policy evaluation system having a first information processing apparatus located on a first site, a second information processing apparatus located on a second site, and a third information processing apparatus located on a third site, the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus stores treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus stores threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus transmits the treated threat data to the first information processing apparatus,

the third information processing apparatus transmits the threat data to the first information processing apparatus,

the first information processing apparatus receives the treated threat data and the threat data,

the first information processing apparatus stores correspondence data which is data indicating correspondence between the threat data and the treated threat data, and

the first information processing apparatus extracts a piece of threat data to which there is no piece of treated threat data corresponding in the received treated threat data, out of the received threat data based on the correspondence data, and generates evaluation data in which the extracted threat data is described.